Applied Cryptography

Fall 2020

- 1. This polynomial is reducible: $p(x) = x^5 + x^4 + 1$. Discover the period(s) of the sequence produced by the LFSR using it as its connection polynomial.
- 2. Prove that $p(x) = x^{10} + x^3 + 1$ is primitive over GF(2).
- 3. Consider the following sequence, and construct the smallest LSFR producing this sequence using the Berlekamp-Massey algorithm: 10011010010000101111101100011111100110